AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computing device comprising:

~~an operating system;~~

a non-volatile memory to store a pre-operating system software program;

a disk memory to store an operating system present software program and an operating system; and

a protected storage medium configured to enable secure exchange of a protected message between the pre-operating system software program ~~to pass an information to~~ and the operating system present software program.

2. (Original) The computing device of claim 1 further comprising:

a first interface to provide the pre-operating system software program access to the protected storage medium; and

a second interface to provide the operating system present software program access to the protected storage medium.

3. (Original) The computing device of claim 1 wherein the protected storage medium is a non-volatile re-writeable memory device.

4. (Cancelled).

5. (Currently Amended) The computing device of claim ~~4~~ 1 wherein the ~~information~~ protected message is ~~passed~~ exchanged during ~~the booting~~ boot-up of the computing device.

6. (Cancelled).

7. (Currently Amended) The computing device of claim ~~6~~ 1 wherein the ~~information is passed during the booting of the computing device~~protected message includes user authentication information.

8. (Cancelled).

9. (Currently Amended) The computing device of claim 1 wherein the protected storage medium is further configured to enable the operating system present software program to

securely ~~pass~~ store the ~~information to~~ protected message for the pre-operating system software program subsequent to boot-up of the computing device.

10. (Currently Amended) The computing device of claim 9 wherein the ~~information~~ protected message is retrieved by the pre-operating system software program ~~after rebooting~~during reboot of the computing device.

11. (Currently Amended) A method comprising:

providing a first interface to a protected storage medium to enable a pre-operating system software program access to ~~the~~ a protected storage medium; ~~and~~.

enabling the pre-operating system software program to perform secure storage of a protected message for the operating system present software program within the protected storage medium; and

providing a second interface to the protected storage medium to enable ~~an~~ the operating system present software program to access ~~to~~ the protected storage medium to enable secure exchange of the protected message between the pre-operating system software program and the operating system present software program.

12. (Currently Amended) The method of claim 11 wherein the protected ~~storage medium is a non-volatile re-writeable memory device~~message includes user authentication information.

13. (Cancelled).

14. (Cancelled).

15. (Currently Amended) The method of claim ~~14~~ 11 wherein ~~enabling~~ providing comprises:

~~enabling the pre-operating system software program to store the information to the protected storage medium; and~~

enabling the operating system present software program to perform secure ~~retrieve~~ retrieval of the ~~information~~ protected message from the protected storage medium.

16. (Currently Amended) The method of claim 15 wherein the ~~information~~ protected message is stored during ~~the booting~~ boot-up of the computing device.

17. (Cancelled).

18. (Currently Amended) The method of claim 11 further comprising:

enabling the operating system present software program to ~~securely pass an information to~~ perform secure storage of a protected request for the pre-operating system software program subsequent to boot-up of the computing device.

A1

19. (Currently Amended) The method of claim 18 wherein enabling comprises:

~~enabling the operating system present software program to store the information to the protected storage medium; and~~

enabling the pre-operating system software program to perform secure ~~retrieve~~ retrieval of the ~~information~~ protected request from the protected storage medium.

20. (Currently Amended) The method of claim 19 wherein the ~~information~~ protected request is retrieved by the pre-operating system software program ~~after rebooting~~ during reboot of the computing device.

21. (Currently Amended) A machine readable medium having instructions stored thereon which when executed by a processor cause the processor to perform operations comprising:

providing a first interface to a protected storage medium to enable a pre-operating system software program access to ~~the~~ a protected storage medium; ~~and~~

enabling the pre-operating system software program to perform secure storage of a protected message for the operating system present software program within the protected storage medium; and

providing a second interface to the protected storage medium to enable ~~an~~ the operating system present software program to access ~~to~~ the protected storage medium to enable secure exchange of the protected message between the pre-operating system software program and the operating system present software program.

22. (Cancelled).

23. (Cancelled).

24. (Currently Amended) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

enabling the operating system present software program to ~~securely pass an information to a second operating system present software program via~~ perform secure retrieval of the protected message from the protected storage medium.

25. (Currently Amended) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

enabling the operating system present software program to perform ~~securely~~ secure storage of ~~pass an information to~~ a protected request for the pre-operating system software program subsequent to boot-up of the device.

Please add the following new claims:

-- 26. (New) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

enabling the pre-operating system software program to perform secure retrieval of the information from the protected storage medium during reboot of the computing device.

27. (New) The method of claim 11 further comprising:

accessing, via the second interface, user authentication information from the protected storage; and

authenticating, by an operating system present user authentication software program, a user according to the user authentication information.

28. (New) The method of claim 11, wherein providing further comprises:

requesting, by a pre-operating system user authentication software program, user authentication information;

accessing, via the first interface, user authentication information from the protected storage;

authenticating, by an operating system present user authentication software program, a user according to the user authentication information;

storing , via the second interface, user authentication information from the protected storage, if the user authentication is successful; and

otherwise, disabling boot-up of a computing device.

29. (New) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

accessing, via the second interface, user authentication information from the protected storage; and

authenticating, by an operating system present user authentication software program, a user according to the user authentication information.

30. (New) The machine readable medium of claim 21 wherein the instructions cause the processor to perform further operations comprising:

requesting, by a pre-operating system user authentication software program, user authentication information;

accessing, via the first interface, user authentication information from the protected storage;

authenticating, by an operating system present user authentication software program, a user according to the user authentication information;

storing , via the second interface, user authentication information from the protected storage, if the user authentication is successful; and

otherwise, disabling boot-up of a computing device. --